

# Phishing und Social Engineering Awareness. Web Based Training.

## Phishing und Social Engineering Awareness. Web Based Training.

 Seminar

 Jederzeit verfügbar

 Teilnahmebescheinigung

 E-Learning

 1 Unterrichtseinheiten

 Online durchführbar

Seminarnummer: 31431

Stand: 19.04.2024. Alle aktuellen Informationen finden Sie unter <https://akademie.tuv.com/s/31431>

In diesem E-Learning erfahren Sie, wie Sie sich vor den aktuell gängigsten Phishing-E-mails und Social-Engineering-Methoden schützen können. Sie werden über verschiedene Arten von Phishing-E-mails informiert und lernen, wie man sie erkennt und bei Angriffen angemessen handelt.

## Nutzen

- Bedrohungserkennung: Teilnehmende lernen, wie sie Phishing-Bedrohungen erkennen und sich im Falle eines Angriffes verhalten sollten, um Daten und Informationen des Unternehmens nicht zu gefährden.
- Die Schulung sensibilisiert die Teilnehmenden bezüglich der aktuellen Gefahrenlage durch Phishing-Mails und zeigt auf, wie Phishing-Attacken erkannt werden.
- Teilnehmende entwickeln die nötige Awareness, um Social-Engineering-Maßnahmen und die dahinterliegenden „psychologischen Tricks“ zu identifizieren.
- Vermeidung von finanziellen Verlusten: Mitarbeitende, die auf Phishing-Angriffe vorbereitet sind, können dazu beitragen, finanzielle Verluste durch Betrug oder Diebstahl von Daten zu vermeiden.
- Stärkung des Unternehmensimage: Eine geschulte Belegschaft kann das Image des Unternehmens als verantwortungsbewusster und sicherer Akteur auf dem Markt stärken.

## Zielgruppe

- Grundsätzlich alle Personen, die sich bzgl. der Bedeutung des Themas „Social Engineering“ und „Phishing-E-mails“ im Rahmen digitaler Kommunikation sensibilisieren möchten.
- Im Speziellen alle Personen, die digitale Endgeräte und Kommunikationsmedien im geschäftlichen Umfeld einsetzen (im Büro, unterwegs oder im Home-Office) und für potenzielle Gefahren, durch

Phishing-Angriffe und Social-Engineering-Taktiken, sensibilisiert werden sollen.

- Branchenübergreifend

## Voraussetzungen

Die Schulung ist für jeden geeignet, der seine Online-Sicherheit verbessern und sich vor Bedrohungen im Internet schützen möchte.

## Inhalte des Seminars

Sie werden über gängige Methoden des Social Engineerings aufgeklärt, mit denen Angreifer und Betrüger versuchen gezielt Menschen zu beeinflussen und zu manipulieren, um beispielsweise Angriffe über Phishing-E-mails erfolgreich durchzuführen.

Am Ende des E-Learnings sind Sie für die Gefahren durch Phishing-E-mails und soziale Manipulation sensibilisiert und tragen durch die neu geschaffene Awareness dazu bei, dass die persönlichen bzw. firmeninternen Informationen und Daten besser geschützt sind.

- Der Faktor Mensch als IT-Sicherheitsrisiko
  - Warum ist der „Faktor Mensch“ für Cyberkriminelle attraktiv?
  - Sicherheitsvorfälle durch menschliches Fehlverhalten
- Social Engineering: Menschen beeinflussen
  - Was ist Social Engineering und wie funktioniert es?
  - Wesentliche Merkmale und Vorgehensweise beim „Social Engineering“
- Was ist Phishing und Spoofing?
  - Abgrenzung und Erklärung der Begrifflichkeiten „Phishing“ und „Spoofing“
  - Allgemeine wiederkehrende Merkmale bei Phishing-Mails
  - Ein Blick auf aktuelle Zahlen
- Die gängigsten Merkmale & Methoden bei Phishing-Mails
  - Spear-Phishing inkl. Praxisbeispiel
  - Clone-Phishing inkl. Praxisbeispiel
  - Dynamite-Phishing inkl. Praxisbeispiel
  - Exkurs: CEO-Fraud (Deepfakes durch KI & Schutz vor dem CEO-Fraud)
- Merkmale von Phishing-E-mails im Detail
  - Wie identifizieren Sie Phishing-Mails?
  - Verdächtige Merkmale im Detail und Praxistipps
  - Ein Blick in die E-Mail: Worauf ist zu achten?
- Phishing-Attacken verhindern
  - Kompakt: Tipps, um Phishing-Angriffe zu erkennen und zu verhindern

# Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter <https://akademie.tuv.com/s/31431> und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.